(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 742 618**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **96 13973**

(51) Int Cl[6] : H 04 L 12/22, H 04 L 9/32

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 15.11.96.

(30) **Priorité** : 17.05.95 KR 9512289.

(43) **Date de la mise à disposition du public de la demande :** 20.06.97 Bulletin 97/25.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

(60) **Références à d'autres documents nationaux apparentés :** Division demand©e le 15/11/96 b©n©ficiant de la date de d©pét du 17/05/96 de la demande initiale nÊ 96 06154

(71) **Demandeur(s) :** *KOREA TELECOM* — KR.

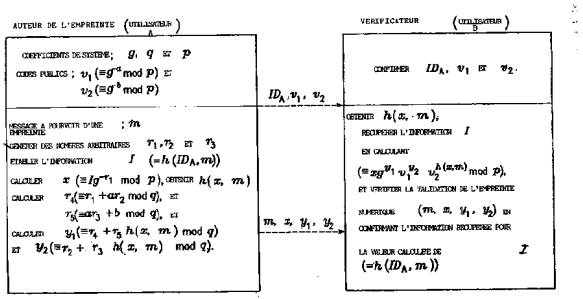
(72) **Inventeur(s) :** AHN KEUM HYUG, LEE YUN HO, PARK ILL HWAN et JANG CHUNG RYONG.

(73) **Titulaire(s) :**

(74) **Mandataire :** CABINET MALEMONT.

(54) SYSTEME D'EMPREINTE NUMERIQUE AVEC APPENDICE.

(57) La présente invention concerne un procédé pour générer une empreinte numérique avec appendice et pour vérifier l'empreinte numérique générée, pour authentifier chaque information de traitement d'identité, protéger l'intégrité de l'information transférée et empêcher le traitement d'informations frauduleuses.



FR 2 742 618 - A1

Système d'empreinte numérique avec appendice

La présente invention concerne un système d'empreinte numérique permettant une récupération de message, et un système d'empreinte numérique avec appendice pour authentifier chaque information de traitement d'identité, protéger l'intégrité de l'information transférée et empêcher le traitement d'informations frauduleuses.

Une empreinte numérique correspondant à une empreinte manuelle classique sert à confirmer un interlocuteur, à empêcher la modification non autorisée du contenu de la communication et à résoudre un litige concernant une attitude de communication. Un procédé destiné à générer l'empreinte numérique peut comprendre un système d'empreinte numérique avec appendice ou un système d'empreinte numérique permettant une récupération de message, suivant les formes et les fonctions de l'empreinte numérique générée.

Si on suppose que p désigne un nombre premier élevé, q un autre nombre premier destiné à diviser p−1, g un entier naturel ayant un reste 1 obtenu grâce à la division de sa puissance q par p, g se situant entre 1 et p, alors g, q et p sont des coefficients de système couramment utilisés par les utilisateurs. Si chaque utilisateur choisit au hasard comme code secret un entier naturel s situé entre 1 et q et utilise comme code public un reste v ($\equiv g^{-s} \bmod p$) obtenu en divisant la puissance −s de g par p, les coefficients publics utilisés par chaque utilisateur sont v, g, q et p.

Il est difficile de trouver le code secret s parmi ces coefficients publics, et un problème de logarithmes discrets est donc difficile à calculer. De nombreux systèmes d'identification de codes publics et de nombreux systèmes d'empreinte numérique sont basés sur le degré de sécurité, du fait que le problème des logarithmes discrets est difficile à calculer.

En 1989, Schnorr a divulgué le système d'identification et le système d'empreinte numérique basés sur la sécurité des logarithmes discrets. Le système d'empreinte numérique divulgué par Schnorr, qui est le système d'empreinte numérique avec appendice, apporte à celui qui avait été divulgué en

1985 par Elgamal une fonction de compression par hachage et simplifie la procédure destinée à générer et à vérifier l'empreinte numérique. De plus, l'empreinte numérique générée est de petite taille.

Le système d'identification proposé par Schnorr utilise la même structure de logarithme que le système d'empreinte numérique, et il authentifie la propre identité d'une personne face à un interlocuteur.

Le système d'identification proposé par Schnorr, selon lequel un fournisseur de preuve A authentifie son identité face à un vérificateur B, va maintenant être décrit.

Si les coefficients de système du fournisseur de preuve sont g, q et p, le code secret s (1 (s < q) et le code public v ($\equiv g^{-s} \bmod p$), le fournisseur de preuve A choisit un nombre arbitraire r situé entre 1 et q et transmet au vérificateur B un reste x ($\equiv g^r \bmod p$) obtenu en divisant la puissance r de g par p. Si x est reçu du fournisseur de preuve A, le vérificateur B choisit un nombre arbitraire e situé entre 1 et q et transmet le nombre e au fournisseur de preuve A. Le fournisseur de preuve multiplie le nombre arbitraire e reçu du vérificateur B par le code secret s et additionne le nombre arbitraire r afin d'obtenir r+se. Le fournisseur de preuve A transmet au vérificateur B un reste y ($\equiv r+se \bmod q$) obtenu en divisant r+se par q. Si y est reçu du fournisseur de preuve A, le vérificateur B calcule un reste x' ($\equiv g^y v^e \bmod p$) obtenu en divisant le produit de la puissance y de g et de la puissance e de v par p. Le vérificateur B authentifie la validation de l'identité du fournisseur de preuve en confirmant que x' et x sont égaux.

Dans le système d'empreinte numérique avec appendice proposé par Schnorr, si un message à pourvoir d'une empreinte est m, l'auteur de l'empreinte A choisit un nombre arbitraire r situé entre 1 et q et calcule un reste x ($\equiv g^r \bmod p$) obtenu en divisant la puissance r de g par p. Le message m et le reste x calculé sont soumis à la fonction de hachage afin d'obtenir e (= h(x, m)). L'auteur de l'empreinte A calcule un reste y ($\equiv r+se \bmod q$) obtenu en divisant r, additionné au produit de s et e, par q. (e, y) est alors l'empreinte numérique avec appendice pour le message m. La validation de l'empreinte numérique (e, y) avec

appendice pour le message m est facilement vérifiée puisqu'on connaît un code public.

Cela veut dire que si l'empreinte numérique avec appendice de l'auteur de l'empreinte A pour le message m est (e, y), le vérificateur B calcule un reste x' ($\equiv g^y v^e \bmod p$) obtenu en divisant le produit de la puissance y de g et de la puissance e de v par p. Le reste x' et le message m sont soumis à la fonction de hachage afin d'obtenir e' (= h(x', m). La validation de l'empreinte numérique (e, y) avec appendice de l'auteur de l'empreinte A est vérifiée grâce à une confirmation que e' et e sont égaux.

Depuis, Nyberg et Rueppel ont divulgué en 1993 le système d'empreinte numérique permettant une récupération de message et basé sur la sécurité des logarithmes discrets. Le système d'empreinte numérique permettant une récupération de message de N-R (Nyberg-Rueppel) va maintenant être décrit.

On suppose que les coefficients de système de l'auteur de l'empreinte sont g, q et p, que le code secret est s ($1 < s < q$), la clé publique v ($\equiv g^{-s} \bmod p$) et le message à pourvoir d'une empreinte m, m étant un entier naturel supérieur ou égal à 1 et inférieur ou égal au nombre premier p. L'auteur de l'empreinte choisit un nombre arbitraire r situé entre 1 et q et calcule un reste x ($\equiv mg^{-r} \bmod p$) obtenu en divisant le produit du message m et de la puissance -r de g par p. L'auteur de l'empreinte additionne r au code secret s multiplié par x afin d'obtenir r+sx, et calcule un reste y ($\equiv r+sx \bmod q$) obtenu en divisant r+sx par q. (x, y) est alors l'empreinte numérique permettant une récupération de message pour le message m.

Pour vérifier l'empreinte numérique (x, y), le vérificateur calcule un reste ($\equiv xg^y v^x \bmod p$) obtenu en divisant le produit de x, de la puissance y de g et de la puissance x de v par p afin de récupérer le message m. Le vérificateur vérifie la validation de l'empreinte numérique (x, y) en confirmant le contenu du message m récupéré.

Cependant, l'empreinte numérique avec appendice génère seulement l'empreinte numérique pour le message. Dans l'empreinte numérique permettant

une récupération de message, si le message à pourvoir d'une empreinte est supérieur en taille à p, le message doit être divisé en différents messages inférieurs à p. Etant donné que l'empreinte numérique est générée pour les messages divisés, cela augmente la taille de l'empreinte numérique générée.

La présente invention a donc pour but de proposer un système d'empreinte numérique avec appendice destiné à confirmer la modification non autorisée d'un message et à détecter le comportement de transmission.

Le but de l'invention est atteint par un procédé pour générer une empreinte numérique avec appendice et pour vérifier l'empreinte numérique générée, lorsque les coefficients de système sont g, q et p, caractérisé par les phases suivantes :

sélection (par l'auteur d'une empreinte) d'un premier nombre arbitraire r1, application d'une fonction de hachage pour un message m et une identification ID de l'auteur de l'empreinte afin d'obtenir h(ID, m), calcul d'un premier reste x ($\equiv h(ID, m)\ g^{-r1} \bmod p$) obtenu en divisant le produit de h(ID, m) et de la puissance –r1 de g par p, et application de la fonction de hachage pour le premier reste x et ledit message m afin d'obtenir h (x, m) ;

sélection d'un deuxième et d'un troisième nombre arbitraire r2 et r3, calcul d'un deuxième reste r4 ($\equiv r1 + ar2 \bmod q$) obtenu en divisant par q le premier nombre arbitraire r1 additionné au produit d'un premier code secret a et du deuxième nombre arbitraire r2, et calcul d'un troisième reste r5 ($\equiv ar3 + b \bmod q$) obtenu en divisant par q un second code secret b additionné au produit du premier code secret a et du troisième nombre arbitraire r3 ;

calcul d'un quatrième reste y1 ($\equiv r4 + r5\ h(x, m) \bmod q$) obtenu en divisant par q le deuxième reste r4 additionné au produit du troisième reste r5 et de h(x, m), et calcul d'un cinquième reste y2 ($\equiv r2 + r3\ h(x, m) \bmod q$) obtenu en divisant par q le deuxième nombre arbitraire r2 additionné au produit du troisième nombre arbitraire r3 et de h(x, m), pour générer ainsi une empreinte numérique (x, y1, y2) pour le message m ;

application (par un vérificateur) de la fonction de hachage pour le premier reste x et le message m afin d'obtenir h(x, m), et récupération de h(ID,

m) grâce au calcul d'un sixième reste ($\equiv xg^{y1}v1^{y2}v2^{h(x,m)} \bmod p$) obtenu en divisant par p le produit du premier reste x, de la puissance y1 de g, de la puissance y2 d'un premier code public v1 ($\equiv g^{-a} \bmod p$) et de la puissance {h(x, ID)} d'un second code public v2 ($\equiv g^{-b} \bmod p$) ; et

vérification de la validation de l'empreinte numérique (x, y1, y2) grâce à la confirmation que la valeur h(ID, m) récupérée est égale à la valeur h(x, ID) obtenue grâce à l'application de la fonction de hachage pour l'identification ID de l'auteur de l'empreinte et le message m.

La présente invention va être décrite plus en détail en référence aux dessins joints.

La figure 1 montre un traitement pour un système d'empreinte numérique permettant une récupération de message selon la présente invention,

la figure 2 montre un traitement pour un système d'empreinte numérique avec appendice selon la présente invention, et

la figure 3 montre un traitement pour un système d'identification selon la présente invention.

Selon la figure 1, chaque utilisateur a deux codes secrets et deux codes publics correspondant à ceux-ci, et peut générer une empreinte numérique pour un message à pourvoir d'une empreinte. Si le message à pourvoir d'une empreinte est m, les codes secrets de l'auteur de l'empreinte a et b et les codes publics v1 ($\equiv g^{-a} \bmod p$) et v2 ($\equiv g^{-b} \bmod p$), chaque utilisateur utilise couramment une fonction de hachage h et des coefficients de système g, q et p. Pendant l'utilisation d'un système d'empreinte numérique, une identification unique (ID) est attribuée à chaque utilisateur à partir d'un centre d'authentification de code.

Un auteur d'empreinte A choisit un nombre arbitraire r1 situé entre 1 et q et calcule un reste x ($\equiv mg^{-r1} \bmod p$) obtenu en divisant le produit du message m et de la puissance −r de g par p. Il soumet le reste x et son identification ID_A à la fonction de hachage afin d'obtenir $h(x, ID_A)$. Il choisit des nombres arbitraires r2 et r3 situés entre 1 et q et calcule r4 ($\equiv r1 + ar2 \bmod q$),

r5 ($\equiv$ ar3 + b mod q), y1 ($\equiv$ r4 + h(x, ID_A)r5 mod q), et y2 ($\equiv$ r2 + h(x, ID_A)r3 mod q).

Au lieu de calculer y1 et y2 en utilisant h(x, ID_A) après avoir choisi r2 et r3 et après avoir calculé r4 et r5 à l'aide des codes secrets a et b, on peut choisir comme valeur de y2 un nombre arbitraire r2 et calculer y1 en utilisant les codes secrets a et b et la valeur calculée pour h(x, ID_A). Cela veut dire que l'auteur de l'empreinte A choisit le nombre arbitraire r2 situé entre 1 et q comme valeur de y2. Puis y1 est calculé à l'aide de la formule y1 $\equiv$ r1 + h(x, ID_A)b + ay2 mod q. La valeur (x, y1, y2) obtenue est donc l'empreinte numérique permettant une récupération de message pour le message m.

Pour vérifier l'empreinte numérique (x, y1, y2), un vérificateur B soumet x et l'identification ID_A de l'auteur de l'empreinte à la fonction de hachage afin d'obtenir h(x, ID_A). On récupère le message m en calculant un reste ($\equiv xg^{y1}v1^{y2}v2^{h(x,IDA)}$ mod p) obtenu en divisant par p le produit de x, de la puissance y1 de g, de la puissance y2 du code public v1 et de la puissance {h(x, ID_A)} du code public v2. Le vérificateur B vérifie la validation de l'empreinte pour le message m en confirmant le contenu du message m récupéré.

Selon la figure 2, l'empreinte numérique générée est ajoutée à la fin d'un message pourvu d'une empreinte et est traitée par paire avec ce message.

L'auteur de l'empreinte A soumet son identification ID_A et le message m à la fonction de hachage afin d'obtenir I (= h(ID_A, m)). Il établit également I en annexant les données relatives à la sécurité, par exemple la description pour le message correspondant et l'heure à laquelle l'empreinte numérique est générée par un terminal d'ordinateur. Il choisit un nombre arbitraire r1 situé entre 1 et q et calcule un reste x ($\equiv Ig^{-r1}$ mod p) obtenu en divisant le produit de I et de la puissance -r1 de g par p. Il soumet x et le message m à la fonction de hachage afin d'obtenir h(x, m). Il choisit enfin des nombres arbitraires r2 et r3 situés entre 1 et q et calcule r4 ($\equiv$ r1 + ar2 mod q), r5 ($\equiv$ ar3 + b mod q), y1 ($\equiv$ r4 + h(x, m)r5 mod q) et y2 ($\equiv$ r2 + h(x, m)r3 mod q).

Au lieu de calculer y1 et y2 en utilisant h(x, m) après avoir choisi les nombres arbitraires r2 et r3 et après avoir calculé r4 et r5 à l'aide des codes

secrets a et b, on peut choisir comme valeur de y2 un nombre arbitraire r2 et calculer y1 en utilisant les codes secrets a et b et h(x, m) : l'auteur de l'empreinte A choisit comme valeur de y2 les nombres arbitraires r2 entre 1 et q. Le reste y1 est calculé à l'aide de la formule $y1 \equiv r1 + h(x, m)b + ay2 \bmod q$. (x, y1, y2) est ainsi l'empreinte numérique avec appendice pour le message m et est traitée avec celui-ci sous la forme (m, x, y1, y2).

Pour vérifier l'empreinte numérique (m, x, y1, y2) avec appendice, le vérificateur B calcule h(x, m) en soumettant x et le message m dans l'empreinte numérique (m, x, y1, y2) à la fonction de hachage. On récupère I en calculant un reste ($\equiv xg^{y1}v1^{y2}v2^{h(x,m)} \bmod p$) obtenu en divisant par p le produit de x, de la puissance y1 de g, de la puissance y2 de v1 et de la puissance (h(x,m)) de v2. Le vérificateur B soumet l'identification ID_A de l'auteur de l'empreinte et le message m à la fonction de hachage afin d'obtenir $h(ID_A, m)$. On vérifie la validation de l'empreinte numérique avec appendice pour le message m en confirmant que la valeur obtenue pour $h(ID_A, m)$ est égale à la valeur récupérée pour I.

En conséquence, l'empreinte numérique permettant une récupération de message et l'empreinte numérique avec appendice sont utilisées d'une manière appropriée en fonction de la longueur de la séquence binaire du message à pourvoir d'une empreinte. Si la taille du message est petite, l'auteur de l'empreinte utilise l'empreinte numérique permettant une récupération de message. Etant donné que le vérificateur peut récupérer le message pourvu d'une empreinte à partir du résultat de la vérification de la validation de l'empreinte numérique, l'importance de la communication entre l'auteur de l'empreinte et le vérificateur peut être réduite. Si la taille du message est grande, l'empreinte numérique avec appendice est utilisée pour générer l'empreinte numérique comprenant des informations comme une phrase de description de l'auteur de l'empreinte, une heure d'empreinte, etc.

Cela veut dire que l'auteur de l'empreinte soumet son identification ID et le message m à la fonction de hachage afin d'obtenir h(ID, m). Il annexe à h(ID, m) la phrase de description pour le message m. Il établit I (= $h(ID_A, m)$, une

phrase de description et une heure d'empreinte) en annexant la description pour le message correspondant et l'heure à laquelle l'empreinte numérique est générée par un terminal d'ordinateur, et génère l'empreinte numérique avec appendice.

Selon la figure 3, pour améliorer la sécurité, chaque utilisateur peut utiliser deux codes secrets et deux codes publics correspondant à ceux-ci. Des nombres arbitraires a et b sont choisis entre 1 et q comme codes secrets. Les codes publics sont v1 ($\equiv g^{-a} \bmod p$) et v2 ($\equiv g^{-b} \bmod p$). Pour prouver sa propre identité à un vérificateur B, le fournisseur de preuve A choisit un nombre arbitraire r1 situé entre 1 et q et calcule la puissance -r1 de g. Le fournisseur de preuve A établit l'information I (= ID_A, date et heure d'empreinte, adresse du terminal utilisé, etc.) contenant son identification ID_A, la date et l'heure d'empreinte, une adresse d'ordinateur central ou une adresse de noeud indiquant une position d'un terminal utilisé, etc., et transmet x ($\equiv Ig^{-r1} \bmod p$) au vérificateur B. L'information d'authentification I peut être 1.

Si x est reçu du fournisseur de preuve A, le vérificateur B choisit un nombre arbitraire e situé entre 1 et q et transmet le nombre arbitraire e au fournisseur de preuve A. Celui-ci soumet e et x à la fonction de hachage afin d'obtenir h(x, e). Les nombres r2 et r3 situés entre 1 et q sont choisis au hasard par le fournisseur de preuve A tandis que r4 ($\equiv r1 + ar2 \bmod q$) et r5 ($\equiv ar3 + b \bmod q$) sont calculés. Le fournisseur de preuve A transmet y1 ($\equiv r4 + h(x, e)r5 \bmod q$) et y2 ($\equiv r2 + h(x, e)r3 \bmod q$) au vérificateur B.

Dans la description précédente, on calcule y1 et y2 en utilisant h(x, e) après avoir choisi les nombres arbitraires r2 et r3 et après avoir calculé r4 et r5 en utilisant les codes secrets a et b. Cependant, on peut choisir comme valeur de y2 un nombre arbitraire r2 et calculer y1 en utilisant a et b et h(x, e) : le fournisseur de preuve A choisit comme valeur de y2 le nombre arbitraire r2 entre 1 et q, et le reste y1 est obtenu grâce à la formule $y1 \equiv r1 + h(x, e)b + ay2 \bmod q$). Le fournisseur de preuve A transmet y1 et y2 au vérificateur B.

Si y1 et y2 sont reçus du fournisseur de preuve A, le vérificateur B récupère l'information d'authentification I en calculant $xg^{y1}v1^{y2}v2^{h(x,e)} \bmod p$. Le

vérificateur B authentifie l'identité du fournisseur de preuve en confirmant le contenu de l'information d'authentification I récupérée.

D'autre part, le nombre arbitraire –r1 peut être utilisé à la place du nombre arbitraire r1.

Comme on l'a décrit plus haut, le service d'information fiable est possible et un interlocuteur peut être efficacement authentifié.

REVENDICATIONS

1. Procédé pour générer une empreinte numérique avec appendice et pour vérifier l'empreinte numérique générée, lorsque les coefficients de système sont g, q et p, caractérisé par les phases suivantes :

sélection (par l'auteur d'une empreinte) d'un premier nombre arbitraire r1, application d'une fonction de hachage pour un message m et une identification ID de l'auteur de l'empreinte afin d'obtenir h(ID, m), calcul d'un premier reste x ($\equiv$ h(ID, m) g^{-r1} mod p) obtenu en divisant le produit de h(ID, m) et de la puissance –r1 de g par p, et application de la fonction de hachage pour le premier reste x et ledit message m afin d'obtenir h (x, m) ;

sélection d'un deuxième et d'un troisième nombre arbitraire r2 et r3, calcul d'un deuxième reste r4 ($\equiv$ r1 + ar2 mod q) obtenu en divisant par q le premier nombre arbitraire r1 additionné au produit d'un premier code secret a et du deuxième nombre arbitraire r2, et calcul d'un troisième reste r5 ($\equiv$ ar3 + b mod q) obtenu en divisant par q un second code secret b additionné au produit du premier code secret a et du troisième nombre arbitraire r3 ;

calcul d'un quatrième reste y1 ($\equiv$ r4 + r5 h(x, m) mod q) obtenu en divisant par q le deuxième reste r4 additionné au produit du troisième reste r5 et de h(x, m), et calcul d'un cinquième reste y2 ($\equiv$ r2 + r3 h(x, m) mod q) obtenu en divisant par q le deuxième nombre arbitraire r2 additionné au produit du troisième nombre arbitraire r3 et de h(x, m), pour générer ainsi une empreinte numérique (x, y1, y2) pour le message m ;

application (par un vérificateur) de la fonction de hachage pour le premier reste x et le message m afin d'obtenir h(x, m), et récupération de h(ID, m) grâce au calcul d'un sixième reste ($\equiv$ $xg^{y1}v1^{y2}v2^{h(x,m)}$ mod p) obtenu en divisant par p le produit du premier reste x, de la puissance y1 de g, de la puissance y2 d'un premier code public v1 ($\equiv$ g^{-a} mod p) et de la puissance {h(x, m)} d'un second code public v2 ($\equiv$ g^{-b} mod p) ; et

vérification de la validation de l'empreinte numérique (x, y1, y2) grâce à la confirmation que la valeur h(ID, m) récupérée est égale à la valeur h(x, ID)

obtenue grâce à l'application de la fonction de hachage pour l'identification ID de l'auteur de l'empreinte et le message m.

2. Procédé pour générer une empreinte numérique avec appendice et pour vérifier l'empreinte numérique générée, lorsque les coefficients de système sont g, q et p, caractérisé par les phases suivantes :

sélection (par l'auteur d'une empreinte) d'un premier nombre arbitraire r1, application d'une fonction de compression par hachage pour un message m et une identification ID de l'auteur de l'empreinte afin d'obtenir h(ID, m), calcul d'un premier reste x ($\equiv h(ID, m)\ g^{-r1} \bmod p$) obtenu en divisant le produit de h(x, m) et de la puissance -r1 de g par p, et application de la fonction de hachage pour le premier reste x et ledit message m afin d'obtenir h (x, m) ;

sélection du deuxième nombre arbitraire r2 entre 1 et q comme valeur de y2, calcul d'un premier reste y1 ($\equiv r1 + h(x, m)b + ay2 \bmod q$) obtenu en divisant par q le premier nombre arbitraire r1 additionné au produit d'un premier code secret a et de y2 et au produit d'un second code secret b et de h(x, m), pour générer ainsi une empreinte numérique (x, y1, y2) pour le message m ;

application (par un vérificateur) de la fonction de hachage pour le premier reste x et le message m afin d'obtenir h(x, m), et récupération de h(ID, m) grâce au calcul d'un sixième reste ($\equiv x g^{y1} v1^{y2} v2^{h(x,m)} \bmod p$) obtenu en divisant par p le produit du premier reste x, de la puissance y1 de g, de la puissance y2 d'un premier code public v1 ($\equiv g^{-a} \bmod p$) et de la puissance {h(x, m)} d'un second code public v2 ($\equiv g^{-b} \bmod p$) ; et

vérification de la validation de l'empreinte numérique (x, y1, y2) grâce à la confirmation que la valeur h(ID, m) récupérée est égale à la valeur h(ID, m) obtenue grâce à l'application de la fonction de hachage pour l'identification ID de l'auteur de l'empreinte et le message m.

2742618

FIG. 1

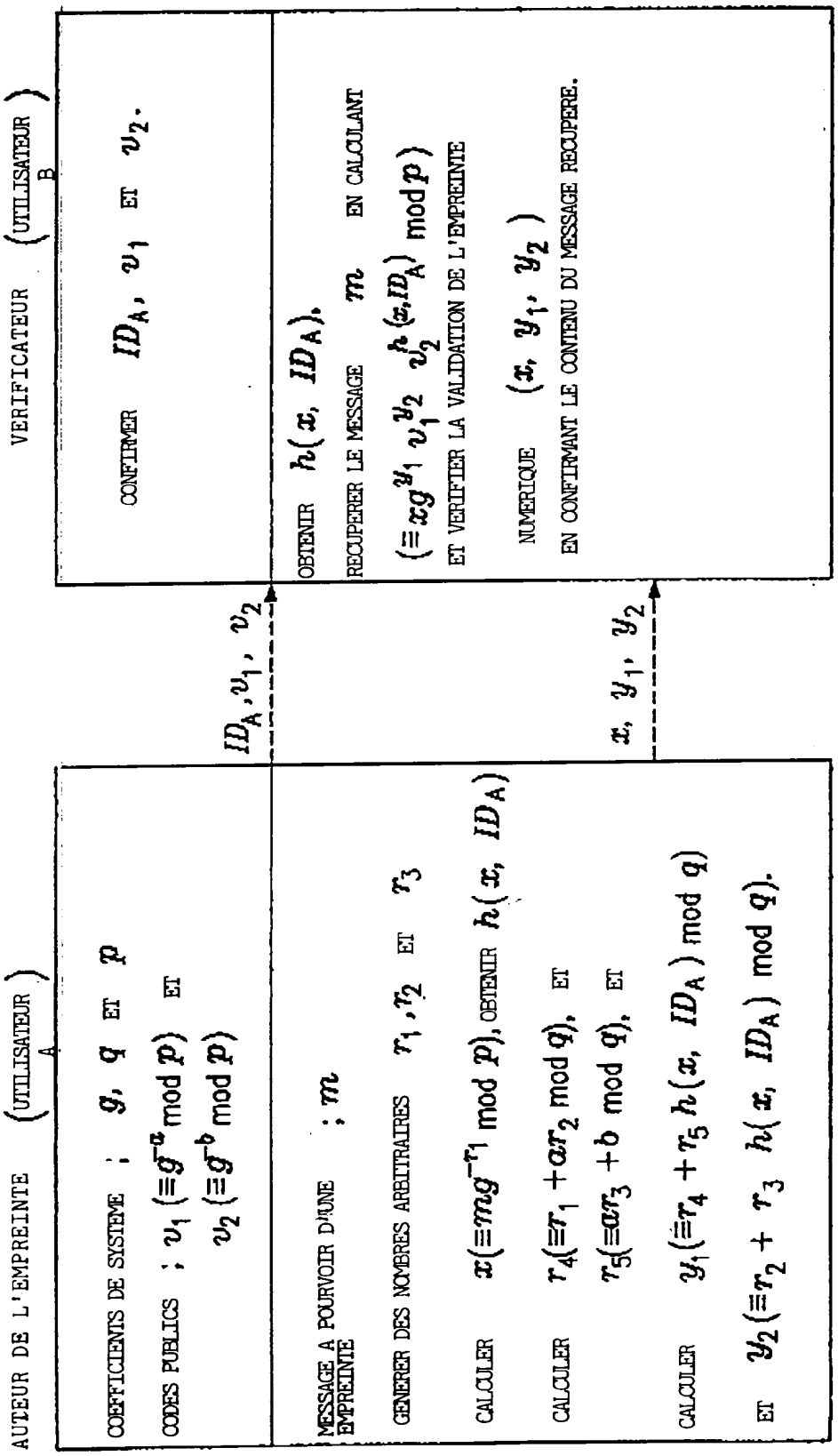
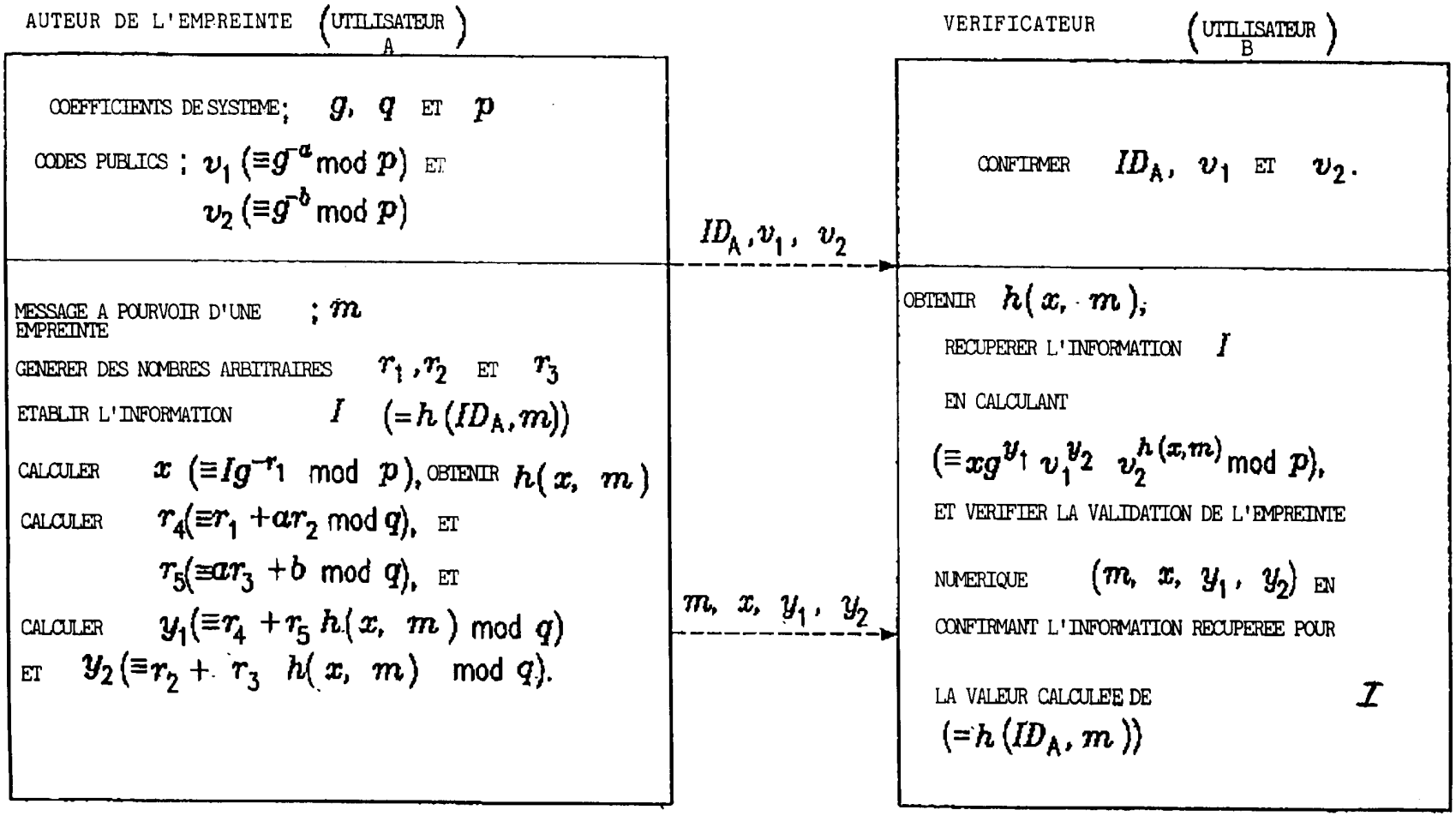
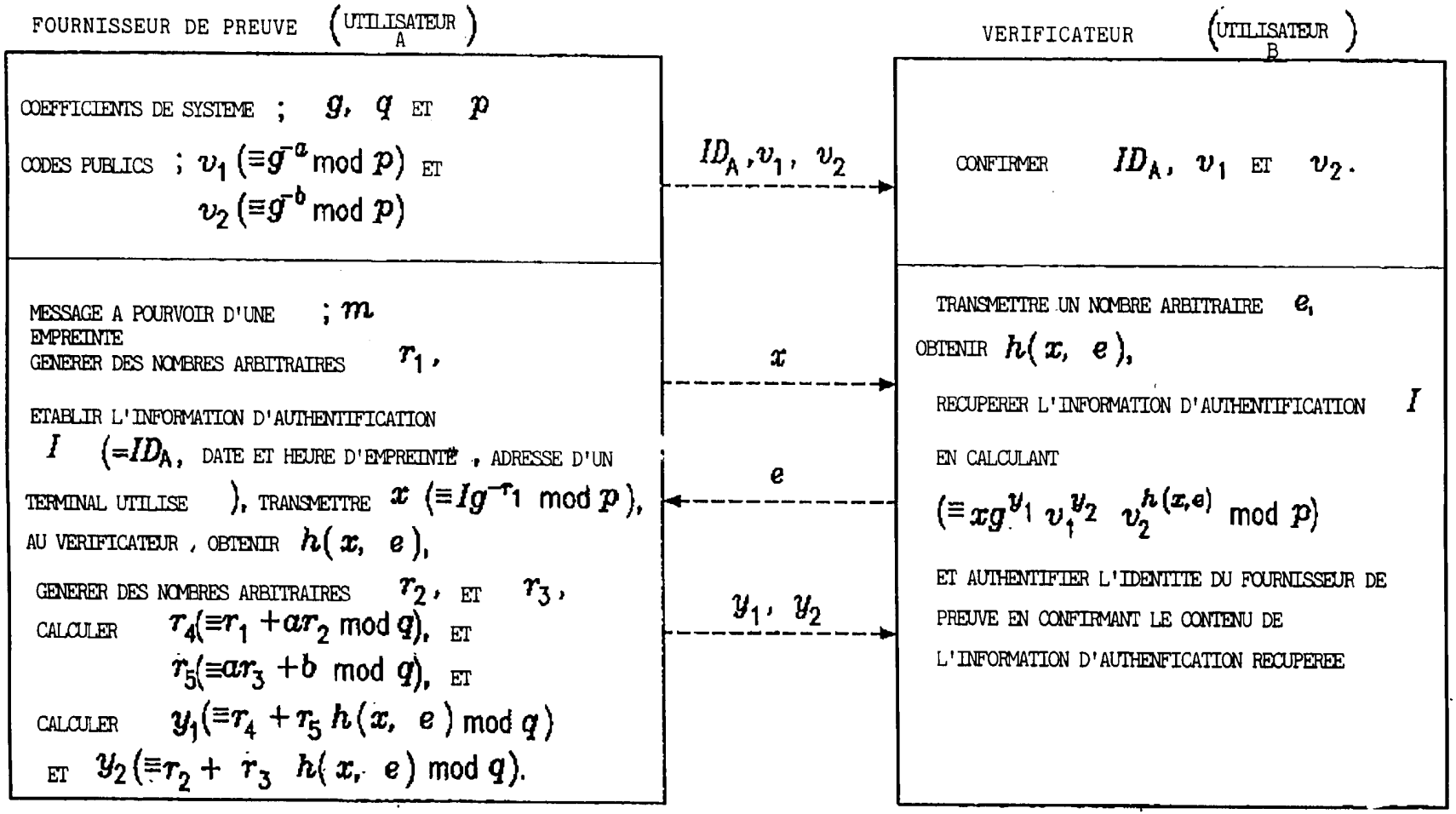


FIG. 2



2742618

FIG. 3



2742618